# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 27-04-2012 | FINAL | |

**4. TITLE AND SUBTITLE**
Son of SPECOPS: Rethinking the Nature and Operationalization of Cyberspace

**5a. CONTRACT NUMBER**
N/A

**5b. GRANT NUMBER**
N/A

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
PHILIP M. FORBES, MAJOR, USAF

Paper Advisor (if Any): CDR JAMES DALTON, USN

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Office of the Provost
Naval War College
686 Cushing Road
Newport, RI 02841-1207

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Distribution Statement A: Approved for public release; Distribution is unlimited.

**13. SUPPLEMENTARY NOTES**: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations. The contents of this paper reflect the author's own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

**14. ABSTRACT**

The establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command under U.S. Strategic Command (USSTRATCOM) signals open acceptance of cyberspace as the newest war-fighting domain. Unlike airpower, however, policy makers and strategists do not have an adequate framework that addresses the nature of cyberspace. Without this understanding, the operationalization of cyberspace beyond broad policy statements and rhetoric will be lacking over the long-term. The alignment of USCYBERCOM under USSTRATCOM is not congruent with the nature of operations in cyberspace and should strive to align itself operationally with USSOCOM.

Despite its joint construct, a reason for the placement of USCYBERCOM under USSTRATCOM remains unclear. USSTRATCOM resembles a clearinghouse of Cold-War era legacy missions or those that are best suited for a conventionally aligned mindset. Conversely, cyber operations present leaders with the imperative to use creativity and initiative to a larger degree than in most other forms of warfare. In such murky philosophical times, guideposts are required that will help direct cyber warfare pioneers toward a direction of "what right looks like". By viewing cyberspace through the lens of special operations policy makers, leaders, and warriors in the cyber field will find lasting success in this new domain.

**15. SUBJECT TERMS**
OPERATIONALIZAITON OF CYBER WARFARE, SPECIAL OPERATIONS, SOF, USSOCOM, USSTRATCOM, USCYBERCOM, POLICY, COLD WAR

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | PHILIP M. FORBES |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 27 | 19b. TELEPHONE NUMBER *(include area code)* 850.865.2590 |

**Standard Form 298 (Rev. 8-98)**

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# Son of SPECOPS:
# Rethinking the Nature and Operationalization of Cyberspace

**by**

**PHILIP M. FORBES**

**Major, USAF**

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**Signature: _____**

**27 APRIL 2012**

**Contents**

## List of Illustrations

**Abstract**

The establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command under U.S. Strategic Command (USSTRATCOM) signals open acceptance of cyberspace as the newest war-fighting domain. Unlike airpower, however, policy makers and strategists do not have an adequate framework that addresses the nature of cyberspace. Without this understanding, the operationalization of cyberspace beyond broad policy statements and rhetoric will be lacking, and planners and strategists will be unable to forge capabilities over the long-term. The alignment of USCYBERCOM under USSTRATCOM is not congruent with the nature of operations in cyberspace and should strive to align itself operationally with USSOCOM.

Despite its joint construct, a reason for the placement of USCYBERCOM under USSTRATCOM remains unclear. USSTRATCOM resembles a clearinghouse of Cold-War era legacy missions or those that are best suited for a conventionally aligned mindset and bureaucratic control despite the global area of interest in which they operate. Conversely, cyber operations present leaders with the imperative to use creativity and initiative to a larger degree than in most other forms of warfare. In such murky philosophical times, guideposts are required that will help direct cyber warfare pioneers toward a direction of "what right looks like". By viewing cyberspace through the lens of special operations and adapting some of its best practices for its own internal use, policy makers, leaders, and warriors in the cyber field will find lasting success in this new domain.

## SCOPE OF THIS PAPER

Much has been published regarding the cyberspace-generated vulnerabilities within the U.S. Government, its infrastructure, and the private sector. Just as nuclear warfare was the Sword of Damocles in the last half of the twentieth century, a reliance on networked information systems has become a necessary, albeit precarious, mainstay of modern existence. Little more discussion is required in this paper on the individual vulnerabilities that lay before us as a connected society, and such specified liabilities are beyond the scope of this work.

Moreover, specific measures to shore up national cyber defenses or to create an offensive cyber capability are discussed in necessarily classified mediums. The same is true with current operations as well as the tactics, techniques, and procedures (TTPs) of special operations forces (SOF). Therefore, with appropriate levels of discussion of paramount importance vis-à-vis classification, the analysis of information gathered via open source information, and the author's personal experiences, have created the pathway for the tacit conclusions and arguments herein.

## INTRODUCTION

After years of advocacy by airpower pioneers such as Billy Mitchell and General Henry "Hap" Arnold, President Harry Truman signed the National Security Act in 1947 that *inter alia* established the U. S. Air Force as an independent Service within the Department of Defense (DOD). The tectonic realignment of the US Army Air Corps into an independent Service constituted an astute policy decision necessary to meet the challenges of command in the face of sweeping changes in technology and its potential to affect warfare for generations. As military airpower continues to thrive in the twenty-first century, cyberspace imperatives now demand that policy makers and strategists confront a new medium in which warfare may be waged and rebirths the same command and control questions that Mitchell, Arnold, and Truman faced.

The establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified component under U.S. Strategic Command (USSTRATCOM) reflects widening recognition of cyberspace as the newest war-fighting domain. Unlike airpower, however, policy makers and strategists do not have an adequate framework by which to address cyberspace's nature. Without such structure, the operationalization of cyberspace beyond broad policy statements and rhetoric will fail, and planners and strategists will be unable to forge capabilities over the long term. USCYBERCOM's alignment under USSTRATCOM is not congruent with the nature of cyberspace operations. Accordingly, this paper proposes that USCYBERCOM align operationally with USSOCOM.

## CURRENT STRUCTURE OF USCYBERCOM

In October 2010, USCYBERCOM reached the full operational capability (FOC) necessary to accomplish its mission of "planning, coordinating, integrating, synchronizing,

and directing activities to operate and defend the Department of Defense information networks and when directed, conduct[ing] full-spectrum military cyberspace operations…in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[1] Much like USSOCOM's Joint Special Operations Command (JSOC), USCYBERCOM coalesces functional components from the U.S. Air Force, Army, Navy, and Marine Corps to fulfill this joint tasking.

Despite its joint construct, however, the placement of USCYBERCOM under USSTRATCOM is functionally puzzling. Similarities among USSTRATCOM components such as tremendous investments in human, financial, and technological capital are what primarily bind the intelligence / surveillance / reconnaissance (ISR), space, and global strike missions with USCYBERCOM. However, in spite of this new tech-heavy component, USSTRATCOM resembles a clearinghouse of missions that are Cold War legacy or best suited for a conventionally aligned mindset and bureaucratic control despite the global area of interest in which they operate.[2] This is not to downplay USSTRATCOM significance or its components because they individually and collectively represent a power-projection capability unmatched anywhere else in the world.

Cyberspace operations occur in a much different operating medium, and require a much different mindset than the coordination of ISR activities, C2 of nuclear weapons, and the positioning of satellites. Described by the DOD as "the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations; global strike; Defense Department information operations; global missile defense; global command,

[1] United States Strategic Command website, "U.S. Cyber Command Factsheet", http://www.stratcom.mil/factsheets/Cyber_Command, Accessed 24 February, 2012.
[2] United States Strategic Command website, "U.S. Strategic Command Snapshot", http://www.stratcom.mil/factsheets/snapshot/, Accessed 24 February, 2012.

control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), and combating WMDs," tethering USCYBERCOM to the confines of this existence blunts its current and potential capabilities.[3] The description implies tacit doctrinal boundaries on its future growth as a medium for war fighting. Such growth in doctrine may be further hampered by leaders within USSTRATCOM who, while acknowledging cyberspace's rapidly changing and fluid environment, are unlikely to have led – and lived – with fleeting opportunities for success in uncertain environments as a way of life. Therefore, cyber capabilities must be unshackled from vintage models of military thinking and leadership.

The unbending checklist discipline of the Cold War, the scientifically discrete and mechanical operations of positioning satellites and the C2 of bombers flying half way around the world perform well within rigorous, regimented processes. In fact, the consequences of not remaining in lock step with rigid guidelines can be disastrous. Such was the case in August 2007, when a B-52 accidentally transported six nuclear-tipped cruise missiles from Minot Air Force Base (AFB), North Dakota, to Barksdale AFB, Louisiana.[4] However, the modern cyber environment – with its dangers and opportunities – presents national security leaders with the imperative to use creativity and initiative to a larger degree than in most other forms of warfare. There is likely no singular "right answer" for creating malware or seeking the origins of a network intrusion. Creating an environment to exercise this latitude requires removing institutional and cultural barriers, and a relinquishing of the military rigidity common to most who serve in uniform. This implies a near-boundless trust be placed upon cyber operators – a trust borne of credibility, integrity, and corporate

[3] U.S. Department of Defense Website,"U.S. Strategic Command Description", http:// www.defense.gov/ orgchart/#60, Accessed February 24, 2012.
[4] Jim Garamone, "Air Force Global Strike Command will Stress Nuclear Mission", American Forces Press Service, August 7, 2009, http://www.af.mil/news/story.asp?id=123162337, Accessed February, 24, 2012.

professionalism, blended with the sought-after technical expertise of a Silicon Valley programmer.

## THE CHALLENGE OF CUTTING LOOSE (BUT NOT TOO MUCH)

Detaching from a conventional military mindset may be difficult given the naturally occurring institutional inertia that plagues senior leaders, such as the Vietnam War in the face of an insurgency. To make the "shackle-breaking" easier, modeling USCYBERCOM after existing organizations will be helpful, but to varying degrees out of DOD reach because of cost and public policy. Nevertheless, private sector examples such as operating environment and leadership climate often contrast with present-day military realities, yet provide a decent vector for pursuing improvements.

Search engine giant Google may well represent the workable model to which USCYBERCOM might aspire. At Google, employee focus is on creative problem solving, innovation, and collaboration. The company headquarters in Mountain View, CA, offer an environment far removed from the culture of physical aptitude and rigidity of the average military base. At Google, it matters little if a programmer can do one hundred push-ups or arrive to work daily with grooming standards "within regs." What matters is the application of talent. Google seeks employees who "thrive in small, focused teams and high-energy environments…and are as passionate about their lives as they are about their work."[5] Furthermore, employees are well compensated with benefits such as on-site laundry service and car washes, free meals on the Google campus, roller hockey, and massage therapy, in addition to the highest average salaries in the tech industry.[6,7] Such benefits are easy to

[5] Google Website, "Google: Jobs: Life at Google", http://www.google.com/intl/en/jobs/lifeatgoogle/index.html, Accessed February 28, 2012.
[6] Google Website, "Google: Jobs: Benefits", http://www.google.com/intl/en/jobs/lifeatgoogle/benefits/index.html, Accessed February 28, 2012.

finance given the singularity of Google's industry focus coupled with its 2011 revenues of $37.9 billion.[8] Unfortunately, to construct such an environment within the DOD is cost-prohibitive.

Between the extremes of existence bounded by USSTRATCOM and Google resides USSOCOM. While the command is best-known as the go-to counter terrorism (CT) solution of policy makers, it is important to appreciate the full landscape of special operations missions. In addition to CT, special operations forces (SOF) perform core tasks depicted in illustration 1.[9] It is important to note that because of the nature of these tasks, USSOCOM has not only grown into an inherently joint combatant command, but one that prizes ingenuity, creativity, innovation, and otherwise unconventional approaches to solving the problems resident in its missions. Such characteristics will attract competent operators to USCYBERCOM. Equally important, they are qualities that leaders of operational cyber units must rouse to properly develop and retain operators.[10]

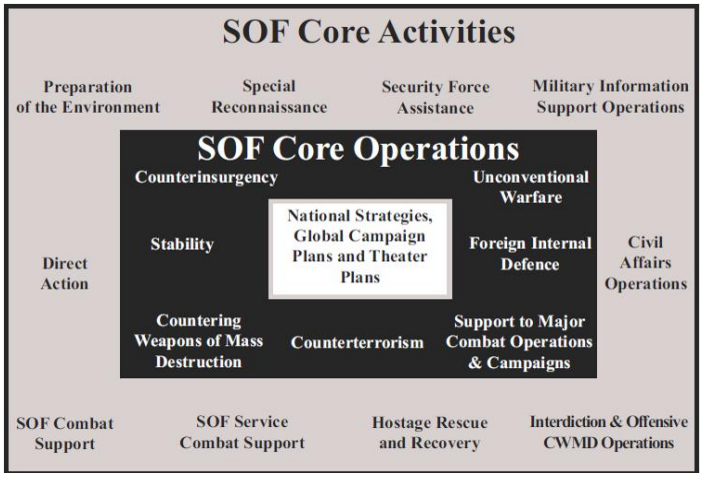

**Illustration 1. SOF Core Activities**

[7] Gus Lubin, "Google Has The Highest Average Salaries In The Tech Industry: $141,000", Business Insider, Jun. 10, 201, http://www.businessinsider.com/google-really-is-the-best-tech-company-to-work-for-2011-6?op=1, Accessed 28 February, 2012.
[8] Securities and Exchange Commission, "Google Filing 10-K for the Fiscal Year Ending 31 December, 2011", December 31, 2011, http://www.sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm, Accessed February 28, 2012.
[9] USUSSOCOM, "U.S. Special Operations Command Factbook: 2012", p.8, October 2011.
[10] For an assessment of personality traits common among Cyber Warriors and the leadership challenges they present, see "Leadership of Cyber Warriors: Enduring Principles and New Directions" by Gregory Conti and David Raymond in the July 11, 2011edition of Small Wars Journal. www.smallwarsjournal.com.

Unclassified reporting of the Global War on Terror (GWOT) highlighted innovations such as USSOCOM forces engaged in counter-terrorism operations partnered with the National Media Exploitation Center (NMEC) to analyze the tremendous volume of computers, thumb drives, and cellphones to extract messages, documents, and names of associates tied to enemy networks.[11] As much of this work involved geographically separated locations participating in the analysis, the need for satellite bandwidth grew. To coordinate the work of analysts and leaders, USSOCOM seized upon the glut of commercial satellite bandwidth that resulted from the dot-com bust, and tied together outstations for distributed information sharing efforts globally.[12] The decentralized execution of war fighting and counter-terrorism persists to this day and USSOCOM continues this stream of innovation. For instance, the command is experimenting with new communications satellites known as "nano-satellites," which have dimensions similar to a loaf of bread, hover in low earth orbit (LEO), and broadcast data directly to fielded SOF command posts.[13]

> *"The Boss [General Stanley McChrystal] would find the 24-year-old kid with a nose ring, with some…brilliant degree from MIT, sitting in the corner with 16 computer monitors humming. He'd say, 'Hey-you…muscle heads couldn't find lunch without help. You got to work together with these guys'"*
> - Major General Mayville in the July 8, 2010 Rolling Stone article *"Runaway General"*

Cyberspace presents challenges that demand the same culture of innovation. The near-exponential improvements in processing power and memory in computing technology, as captured by Moore's Law, constitute the guideline for development in the computing and

[11] Dana Priest, William M. Arkin, "The Vast and Expansive US Secret Army", Washington Post, 2 September, 2011.
[12] Ibid.
[13] John D. Gresham. "SOCOM Year in Review: Completing the Circle", June 27, 2011. http://www.defensemedianetwork.com/stories/socom-year-in-review. Accessed 19 February, 2012

electronics industry since its 1965 inception.[14] This growth in capability has moved in stride with access to technology. From 2000 to 2011, worldwide use of the Internet grew by 528.1 percent.[15,16] In developing areas such as Africa and Latin America, this grew by 2,988.4 and 1,205.1 percent, respectively.[17] In approximately the same period of time (1998 – 2008), trade between these regions and the U.S. grew by 221% and 81 percent respectively.[18,19] In combination, these statistics illustrate the speed at which cyber operations capabilities can and must advance.

The middle ground that USSOCOM provides also properly addresses stakeholder interests vis-à-vis policy and law. Powerful tech firms such as Google have a sea of shareholders and a board of directors whose fiduciary duty is to seek the most profitable outcomes for the company. Missteps in the design or execution of products and services, while unpleasant, typically only damage a company's earnings and do not alter the security of national interests. By contrast, USCYBERCOM serves the U.S. citizenry as the launch pad for digital instruments employed in the best interests of the national policy; the outcomes of command employment have geo-political reverberations.

Indeed, USSOCOM grapples with this reality as well, revealing how tactical actions reap strategic consequences, as the 1993 "Black Hawk Down" incident illustrates. It was, after all, the fallout from this tragic episode that influenced the decision not to intervene in

[14] Michael Kanellos, "Moore's Law to Roll on for Another Decade", CNET News, February 10, 2003. http://news.cnet.com/2100-1001-984051.html. Accessed 20 February, 2012.
[15] Internet World Stats: Usage and Population Statistics."Internet Usage Statistics: The Internet Big Picture", http://www.internetworldstats.com/stats.htm. Accessed 19 February, 2012.
[16] Ibid.
[17] Ibid.
[18] J. F. Hornbeck, "U.S.-Latin America Trade: Recent Trends and Policy Issues", Congressional Research Service, February 8, 2011. http://www.fas.org/sgp/crs/row/98-840.pdf. Accessed February 19, 2012.
[19] As these areas are often characterized by instability, corruption, and criminal activity, a potential expansion of the mission of USUSCYBERCOM exists. Such expansion may include partnering with governments and non-governmental organizations (NGOs) to ensure that global allies in defense and commerce can maintain the network architecture that facilitates daily social and governmental functions. These missions may resemble current USSOCOM role of foreign internal defense (FID).

the 1994 Rwandan genocides.[20] Given such cause and effect, it is appropriate to expect that such asymmetric power exerted in high-stakes operations be governed by policy in spite of the unorthodox and agile nature of both cyber and special operations (SO). In both realms, policy must address legal, moral, ethical, and political impacts of applying capabilities, while simultaneously not confining the military operator to the same modalities of a Missileer in an intercontinental ballistic missile (ICBM) silo.

By viewing cyberspace through the SO lens, and by adapting some of its best practices for its own internal use, policy makers, leaders, and warriors in the cyber field will find true success in this new domain. Given thorough analysis, this viewpoint is within reach. Cyber operations and SO share significant similarities in terms of the nature of the people who practice their tradecraft and the domains in which they exercise it.

## PARALLELS OF OPERATIONAL EXISTENCE

Operationalizing the cyber domain requires in-depth qualitative assessments of both the environment and the personnel who operate within it. Furthermore, to make the case that USCYBERCOM resembles a philosophical twin of USSOCOM requires exploration of the parallels that exist between cyber and SOF activities. No other form of military operations comes as close to intersecting the SO world as does cyberspace.

First among these similarities is that cyber operations, like SO, are rarely a strategically decisive means unto themselves, but are used to complement other military operations in pursuit of higher-level objectives. Modern special operations represent a strategy of cumulative victories in a given campaign, such as the systematic dismantling of

[20] Scott Baldauf, "Why the U.S. Didn't Intervene in the Rwandan Genocide",The Christian Science Monitor, April 7, 2009, http://www.csmonitor.com/World/Africa/2009/0407/p06s14-woaf.html. Accessed February 29, 2012.

Al-Qaeda and its associated movements (AQAM) through capture/kill missions that ultimately led to the killing of Osama bin Laden. Terrorism, however, remains a global threat in spite of this monumental victory. Likewise, the cyber operation involving the Stuxnet malware attack against Iranian nuclear facilities in 2010 has only delayed progress in Iran's nuclear program, not eliminated it.[21] This delay, however, has provided policymakers both the time and diplomatic breathing room to assess Iran's true intentions and design an appropriate response to its potential weapons of mass destruction (WMD) program.

A second parallel is the inherently covert or clandestine nature of both special operations and cyber operations. Special operations forces act as a force multiplier in support of conventional operations or other policy mechanisms, and are trained to conduct sensitive missions in hostile and contested areas.[22] In order to accomplish their assigned missions, SOF must work with speed, precision, and stealth. Similarly, operations in cyberspace possess built-in clandestine properties that make the origins of an attack particularly challenging to trace. A cyberspace operation, for instance, may originate from a suburban home in Virginia Beach, VA, but travel at the speed of light across multiple geographic combatant command (GCC) theaters, through several routers and botnets, slipping through network protocols, and leave in its wake a signature indicating its origin as a Ukraine hospital server. Such anonymity has made tracing the true origins of the 2008 cyber attack on the Georgian government difficult. In spite of media consensus indicating Russian

[21] William J. Broad, et.al, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", New York Times, January 15, 2011,http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Accessed February 14, 2012.
[22] US Department of Defense, "1995 Annual Defense Report, Part VI: Special Operations Forces", 1995. http://www.dod.mil/execsec/adr95/sof_5.html. Accessed January, 27, 2012.

governmental involvement, little evidence exists to prove this beyond doubt.[23] However, cyber operations share more in common with SOF than a shadowy existence of cumulative effects.

**SOF TRUTHS**

- **Humans are more Important Than Hardware.**
- ***Quality* is Better than *Quantity*.**
- **Special Operations Forces Cannot be Mass-Produced.**
- **Competent Special Operations Forces Cannot be Created after Emergencies Occur.**
- **Most Special Operations Require Non-SOF Assistance.**

**Illustration 2. The Five SOF Truths.**

In addition to the defining relationships discussed above, one must also examine the philosophical, SOF operational beliefs that are ingrained into the operator during or shortly after indoctrination. Known as the "SOF Truths," these five principles encompass the unique nature of special operations and apply to the development and understanding of cyber forces and their limitations.

*1) Humans are more important than hardware.*

No amount of specialized weaponry or communications capability can deliver success in the SO world without competent individuals mastering them. USSOCOM places a premium on maturity and experience in the recruiting and development of its SOF operators. This is because many operations occur in locations and situations characterized by volatility, uncertainty, complexity, and ambiguity (VUCA).[24] It is imperative that operators understand not only the operational environment, but also the political implications and the long-term effects of their work.[25] The same holds true for cyber operations. USCYBERCOM may have the physical infrastructure in terms of hardware and software that allows for both

[23] Eneken Tikk, et.al, "Cyber Attacks Against Georgia: Legal Lessons Identified (NATO Unclassified)", Version 1.0. p.12, Cooperative Cyber Defence Centre of Excellence, November 2008. http://www.carlisle.army.mil/DIME/ documents/Georgia%201%200.pdf

[24] Judith Hicks Stiehm and Nicholas W. Townsend (2002), "The U.S. Army War College: Military Education in a Democracy", Temple University Press. p. 6.

[25]. US Army Special Operations Command (USASOC) website, "SOF Imperatives", http://www.soc.mil/USASOC%20Headquarters/SOF%20Imperatives.html. Accessed January 27, 2012.

offensive and defensive operations; however, absence of competent individuals to employ these systems will blunt sustained success. Cyber operators must be capable of interpreting opportunities, weaknesses, and implications in their domain just as SOF must understand the political ramifications of directly or indirectly applying their tradecraft.

*2) Quality is better than quantity*.

To become a member of the U.S. Army Green Berets, candidates undergo a year-long process that includes preparatory introduction, assessment and selection courses, the qualification course (known as the "Q Course"), and live environment training.[26] The result is a culturally aware and mentally agile individual, properly trained to operate in volatile and uncertain environments. Such careful selection and grooming is also required of the cyber warrior. Although cyber operations may not be as physically demanding as SO, the mental challenges of this domain require a highly intelligent operator capable of solving intense problems in complex environments. Furthermore, cyber operators must possess a high level of technical expertise and, perhaps most importantly, a desire to continuously build on their proficiency to meet the demands of rapidly changing technologies, methods, and operational restraints.

In terms of force protection, the careful selection of cyber warriors is on par with the careful screening of potential SOF operators. Special operations units give their applicants, including those in staff functions, a battery of IQ and personality profile tests.[27] These are intended to ensure that not only can individuals perform the tasks required of them, but that they pose no risk to the security of the mission in terms of physical compromise or the

[26] U.S. Army Website: Special Forces. http://www.goarmy.com/special-forces/training.html. Accessed 15 February, 2012.

[27] Author's personal experience.

leaking of sensitive information. Operationalizing cyberspace requires a niche technical expertise known only to a fraction of the Earth's population. With this expertise and access comes both great power and responsibility. Therefore, personnel operating cyber warfare instruments must always act with integrity regardless of the ease with which they can expose sensitive plans or network vulnerabilities for personal or third party gain. Traditional security measures may easily overlook such actions. It follows that a fundamental tenet of developing the capabilities USCYBERCOM needs to operate in the cyber domain with any degree of dominance and security rests primarily on the careful selection of cyber operators.

*3) Special operations forces cannot be mass-produced.*

As a corollary to the foregoing truths, the development of both special operators and cyber operators cannot be set to a lowest common denominator. As such, a limited pool of potential exists from which to recruit. This number decreases through the selection, assessment, and training evolutions that potential operators undergo. No template facilitates the development of all candidates into competent operators. Performance standards are high and not all personality types, regardless of intelligence, can be molded to conduct effective operations in the cyber domain.

This axiom also applies to the instruments of cyber operations. The development of malware, for instance, is contingent on the discovery and exploitation of software. Such ventures imply an investment of time for engineering and testing. Furthermore, once detected, protection measures against this intrusion will likely be developed to prevent further attacks. Because of this, there may only be a limited number of ways in which to exploit a particular system, requiring cyber operations to be uniquely tailored to a particular situation or system.

*4) Competent special operations forces cannot be created after emergencies occur.*

In terms of both personnel and capabilities, this tenet exemplifies the need for continuous development of special and cyber operators, and the constant readiness that allows operators to tackle any number of special operations or cyber operations tasks on short notice. Just as previously discussed tenets espouse the careful selection and training of SOF and cyber warriors, leaders must seek the operator depth of expertise that can accomplish critical mission tasks. Within the cyber domain, such key tasks might include network exploitation, distributed denial of service (DDOS), counter-intelligence, espionage, and social engineering with both offensive and defensive intentions in mind. Regardless of the tasks, one operational factor unifies them all: competence in their execution requires time to develop.

*5) Most special operations require non-SOF assistance.*

Core special operations tasks often require the leveraging of capabilities that are resident in conventional military and interagency (IA) organizations such as the Department of State (DOS), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA). For instance, a team conducting a direct action mission in Africa may require access to a country in order to set up a forward support base (FSB) from which to stage operations. This access may normally be negotiated through diplomatic agreements worked though DOS channels. The same mission may require the transport of SOF personnel and equipment into the target operating area from thousands of miles away, necessitating mobility air force (MAF) assets such as C-17s. While on task, SOF commanders may receive intelligence updates from airborne assets belonging to a coalition partner.

The non-SOF assistance tenet is equally characteristic of operations in the cyber domain because the cyber vulnerabilities resident in American infrastructure, industry, and government networks represent problems that cannot be solved exclusively by DOD personnel. For instance, the current USCYBERCOM mission is to protect DOD information systems; however, defense of the civilian information grid rests with the Department of Homeland Security (DHS).[28] Given that access to government and civilian information systems is available to a hacker of sufficient talent, from a single terminal, malware attacks and probes may require a two-pronged defense from DHS and the DOD. Likewise, a targeted attack against a terrorist network's financial pathways may come at the request of, or through close coordination with, a host nation. Development of malware to inflict damage may come about from collaboration with experts in the private sector and any consequence management required after its use may be handled via non-DOD channels.

The Stuxnet malware attack on Iranian nuclear facilities illustrates this cooperative relationship. From the viewpoint of defense, information security company Symantec reverse engineered the malware in a forensic attempt to determine its origins.[29] This instance alludes to a potential avenue to perform forensic analysis on cyber attacks by leveraging private sector expertise in the future, especially where such capability exceeds that which resides within USCYBERCOM. In the offensive sense, the very construction of the Stuxnet worm appears to have been collaborative as it represents a "Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community (rather) than the likely product of a dedicated, autonomous, advanced research programme

[28] Siobhan Gorman and Yochi Dreazen, "Military Command is Created for Cyber Security", The Wall Street Journal, 24 June, 2009.

[29] James P. Farwell, Rafal Rohozinski,"Stuxnet and the Future of Cyber War". Survival, Vol.53, Issue 1. P. 23. January, 2011.

[*sic*] or 'skunk works.'"[30] This statement epitomizes the habitual working relationships that USCYBERCOM will have to build with other governments, interagency organizations, and the private sector to properly tailor operational effects in the face of increasing complexity and fluidity within the cyber domain.

## COUNTER-ARGUMENT

Proponents of maintaining CYBERCOM's philosophical *status quo* may argue that cyberspace operations, particularly the militarized application of cyber tools against an opponent, are too strategically important to model the character of USSOCOM. True, innovation must occur at a rapid pace, but a culture of latitude and initiative down to the lowest level is not appropriate at this stage in the development of cyber warfare and the policies that govern its use. USSTRATCOM possesses the correct climate and mix of leaders who have historically managed the planning and application of such highly valued instruments of warfare, unique to few countries in the world, and so capable of tipping the balance of power. USCYBERCOM, indeed, possesses such capabilities and promise. Therefore, some analysts argue, it is perhaps best for USCYBERCOM to remain culturally and administratively aligned under USSTRATCOM.

In response to such argument, it is fair to assert that the initial placement of USCYBERCOM under USSTRATCOM made sense, *prima facie*, and allowed it to stand up and reach FOC in an effective process. However, as policy makers and military leaders recognize the operational nature of the cyber domain to be well beyond merely defending DOD computer networks, it is imperative that USCYBERCOM "grow" its institutional

[30] Ibid.

culture, leadership, and doctrine to accommodate its operational environment.[31] The modern world presents USCYBERCOM with examples and avenues that provide accurate vector to an operational ethos; however, most examples lay within the technology sector of private industry. Within the DOD, however, the character of special operations warfare and the talent that USSOCOM continuously recruits and develops provides the example that USCYBERCOM should emulate.

As Shakespeare's Juliet appealed in asking, "What's in a name?", there are apt reasons to categorize cyber operations alongside special operations. Joint Publication 3-05 answers this question by describing SO as those that "can be tailored to achieve not only military objectives through application of SOF capabilities for which there are no broad conventional force requirements, but also to support the application of the diplomatic, informational, and economic instruments of national power".[32] The nature of cyber operations infers this as well. For instance, it would be difficult for myriad reasons to bomb the infrastructure of the Iranian nuclear program with much of it dispersed about the country, well defended, and buried deep underground. Stuxnet, however, crippled Iran's nuclear program without a single aircraft, ship, or soldier crossing the Iranian border. Cyber operations have the potential to reach opponents beyond the grasp of traditional military applications. A caveat to cyber operations, however, is that the environment in which they are applied is ever changing and crowded by the potential for cyber collateral damage, yet asymmetrically capable of leveraging power in pursuit of national objectives.

---

[31] Section 954 of the 2012 NDAA acknowledges USCYBERCOM's offensive cyber role: "Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. 1541 et seq.). U.S. Congress, ''National Defense Authorization Act for Fiscal Year 2012'', Washington D.C, January 5, 2011, Sec. 954.

[32] "Joint Publication 3-05: Joint Special Operations", p.I-1, U.S. Special Operations Command, April 18, 2011.

While we must accept that cyber operations are not of the same species as global strike or ISR mission sets, but of special operations, so too must we adapt the mindset that special operations are more than what the past ten years of warfare has left as a prevailing impression. Special operations involve more than a team of commandos landing outside a compound in Afghanistan and conducting a direct action mission. In fact, such actions on the objective represent several hours of joint, inter-agency forensic analysis and target development that has made the SOF role in manhunting so successful. It is in this vein that we can view the operationalization of cyberspace: the culmination of habitual joint, inter-agency, relationships whose success is realized only after extensive examination of a problem and the myriad pathways to solve it. Moreover, just as with SO, cyber operations must be executed by talented individuals possessing the tactical latitude to employ the cyber tradecraft professionally, and in accordance with self-realized doctrine.

## RECOMMENDATIONS

In light of the parallels resident in the SO and cyber environments, it seems practical that USCYBERCOM undergo one of two possible changes. The first would be an external reorganization under USSOCOM. In lieu of the first option, the second best course of action is to open both USCYBERCOM and USSOCOM for personnel exchanges and liaison duty.

The realignment of USCYBERCOM as a sub-unified command under USSOCOM would resemble shift similar to the establishment of the Air Force as an independent Service. In the Air Force case, a tremendous cultural leap enabled the autonomous development of airpower doctrine unencumbered by a parent organization whose interests remained tethered to the ground or maritime environments. Positioning USCYBERCOM under USSOCOM would place it under the aegis of a parent organization whose ethos is influenced heavily by

the peculiar environment and circumstances in which it operates – an environment that closely resembles what cyber warriors, their leaders, and policy makers are beginning to understand. It follows that cyber doctrine will continue to be shaped not only by national policy but also by looking through a shared operational lens, continuously bringing all things VUCA into view.

Furthermore, this realignment will be most helpful in taking USCYBERCOM "outside the conventional [acquisition] system for major long-term weapons systems" as was called for by Undersecretary of Defense for Acquisition, Technology and Logistics, Frank Kendall.[33] Placing USCYBERCOM under USSOCOM will ensure this non-standard domain receives non-standard methods of employing cyber tradecraft. A spirit of rapid innovation, borne of a SOF heritage and fused with the technical expertise of carefully selected cyber operators, is vital to this.

A second, less disruptive, change may also be a means to preempt a wholesale realignment of USCYBERCOM under USSOCOM. The cross-flow of personnel between USCYBERCOM and components of USSOCOM will effectively braid the operational understanding of both spheres of warfare into an existence of habitual interaction. To be sure, SO may require a cyber solution to assist in solving a particular problem in the future. Likewise, operators within USCYBERCOM will benefit from a seasoned SOF perspective embedded within its planning or operations staffs, or even assuming leadership roles and vice versa. Moreover, these exchanges need not be confined to permanent changes of station (PCS) but may be of a temporary nature such as a USCYBERCOM operator deploying to a

[33] David Fulghum, "Cybercost Control: Industry Disallowed from Tacking Cybertheft Losses onto Pentagon Programs", Aviation Week & Space Technology, p.54, February 27, 2012.

theater special operations command (TSOC) to assist in the planning of special operations missions.

Of paramount importance, these departures from an operator's typical career path must not come as a detriment to the individual's chances for advancement, but as an enhancement. This is easiest to accomplish through institution-wide understanding of the mutual benefits and operational parallels of both special and cyber operations. Such an understanding evolves through the inclusion of both SOF and cyber forces in bilateral and multilateral training events, exercises, and real-world operations (especially during the development of plans and staff estimates). By eliminating such pitfalls, both commands will be able to attract the most talented individuals available for exchange.

## CONCLUSIONS

Dawn illuminates a new form of warfare. National and military leaders, certain of its gravity as an instrument of policy, have appropriately planted the seeds to operationalize the cyber domain. In coming to terms with the nature of cyber operations, as well as its potential to alter the very character of warfare, the development of cyber doctrine and the conduct of militarized cyber activities require scrutiny. Just as airpower challenged the institutional prestige of sailors and infantrymen during its advent, the capability to conduct and defend against hostile acts over computer networks sets the existence of USCYBERCOM apart from all other Services and their components. Institutional mindsets across the DOD and among policymakers are often difficult to transform even while confronting such a revolution in military affairs that parallels the opening chapters of military aviation. In such murky philosophical times, guideposts are required that will help direct cyber warfare pioneers toward a direction of "what right looks like." Such guideposts exist in places like Hurlburt

Field, Fort Bragg, Coronado, and more importantly, in the intrepid spirits of the SOF who live and deploy from there.

## SELECTED BIBLIOGRAPHY


United States Department of Defense. *U.S. Strategic Command Description*. 24 Feb. 2012. Accessed February 24, 2012. http:// www.defense.gov/orgchart/#60.

Baldauf, Scott. *Why the U.S. Didn't Intervene in the Rwandan Genocide*. The Christian Science Monitor. 7 Apr 2009. Accessed 29 Feb. 2012 http://www.csmonitor.com/World/Africa/2009/0407/p06s14-woaf.html.

Broad, William J. *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. New York Times 15 Jan 2011. Accessed 14 Feb. 2012 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Conti, Gregory and David Raymond. *Leadership of Cyber Warriors: Enduring Principles and New Directions*. Small Wars Journal. 11 July 2011. Accessed 24 Feb 2012 http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions.

Farwell, James P and Rafal Rohozinski. *Stuxnet and the Future of Cyber War*. Survival 53. 1 Jan 2011. pp.23-40. Accessed 24 Feb 2012. http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586.

Fulghum, David. *Cybercost Control: Industry Disallowed from Tacking Cybertheft Losses onto Pentagon Programs*. Aviation Week & Space Technology. 27 Feb 2012. Accessed 27 Feb 2012. http://ebird.osd.mil/ebird2/ebfiles/e20120227872090.html.

Garamone, Jim. *Air Force Global Strike Command will Stress Nuclear Mission*. 7 Aug 2009. Armed Forces Press Service. Accessed 24 Feb 2012 http://www.af.mil/news/story.asp?id=123162337.

Google. *Google Jobs*. Accessed 28 Feb 2012 http://www.google.com/intl/en/jobs/.

Gorman, Siobhan and Yochi Dreazen. *Military Command is Created for Cyber Security*. The Wall Street Journal. 24 June 2009. Accessed 24 Feb 2012. http://online.wsj.com/article/SB124579956278644449.html.

Gresham, John D. *SOCOM Year in Review: Completing the Circle*. Defense Media Network. 27 June 2011. Accessed 19 Feb. 2012. http://www.defensemedianetwork.com/stories/socom-year-in-review.

Hornbeck, J F. *U.S.-Latin America Trade: Recent Trends and Policy Issues*. Congressional Research Service. 8 Feb 2011. Accessed 19 Feb 2012. http://www.fas.org/sgp/crs/row/98-840.pdf.

Internet World Stats. *Internet Usage Statistics: The Internet Big Picture.* 19 Feb. 2012. http://www.internetworldstats.com/stats.htm.

Kanellos, Michael. *Moore's Law to Roll on for Another Decade*. CNET News. 10 Feb. 2003. Accessed 20 Feb 2012. http://news.cnet.com/2100-1001-984051.html.

Lubin, Gus. *Google Has The Highest Average Salaries In The Tech Industry: $141,000.* Business Insider. 10 June 2011.
http://www.businessinsider.com/google-really-is-the-best-tech-company-to-work-for-2011-6?op=1

Priest, Dana and William M. Arkin. *The Vast and Expansive US Secret Army*. Washington Post. 2 Sept 2011.
http://readersupportednews.org/news-section2/323-95/7284-the-vast-and-expansive-us-secret-army

Stiehm, Judith H and Nicholas W. Townsend. *The U.S. Army War College: Military Education in a Democracy*. Diss. Temple Univeristy Press. 2002.

Tikk, Eneken. *Cyber Attacks Against Georgia: Legal Lessons Identified (NATO Unclassified).* Cooperative Cyber Defence Centre of Excellence. Nov 2008: 12. Cooperative Cyber Defence Centre of Excellence.

U.S Government. Department of Defense. *1995 Annual Defense Report, Part VI: Special Operations Forces*. 1995. http://www.dod.mil/execsec/adr95/sof_5.html

U.S. Government. Securities and Exchange Commission. *Google Filing 10-K for the Fiscal Year Ending 31 December, 2011*. New York. 31 Dec. 2011.

U.S. Government. U.S. Congress. *National Defense Authorization Act for Fiscal Year 2012''*. Washinton, D.C. 5 Jan 2011.

U.S. Government. U.S. Special Operations Command. *Joint Publication 3-05: Joint Special Operations*., 18 Apr 2011.

U.S. Special Operations Command. *U.S. Special Operations Command Factbook: 2012*. Tampa, 2012.

United States Strategic Command,. *U.S. Cyber Command Factsheet*. Accessed 24 Feb 2012. http://www.stratcom.mil/ factsheets/Cyber_Command.

US Army Special Operations Command. *SOF Imperitives*. Accessed 27 Jan 2012 http://www.soc.mil/ USASOC%20Headquarters/SOF%20Imperatives.html.

US Army. *Special Forces*. Accessed 15 Feb 2012 <http://www.goarmy.com/special-forces/training.html